

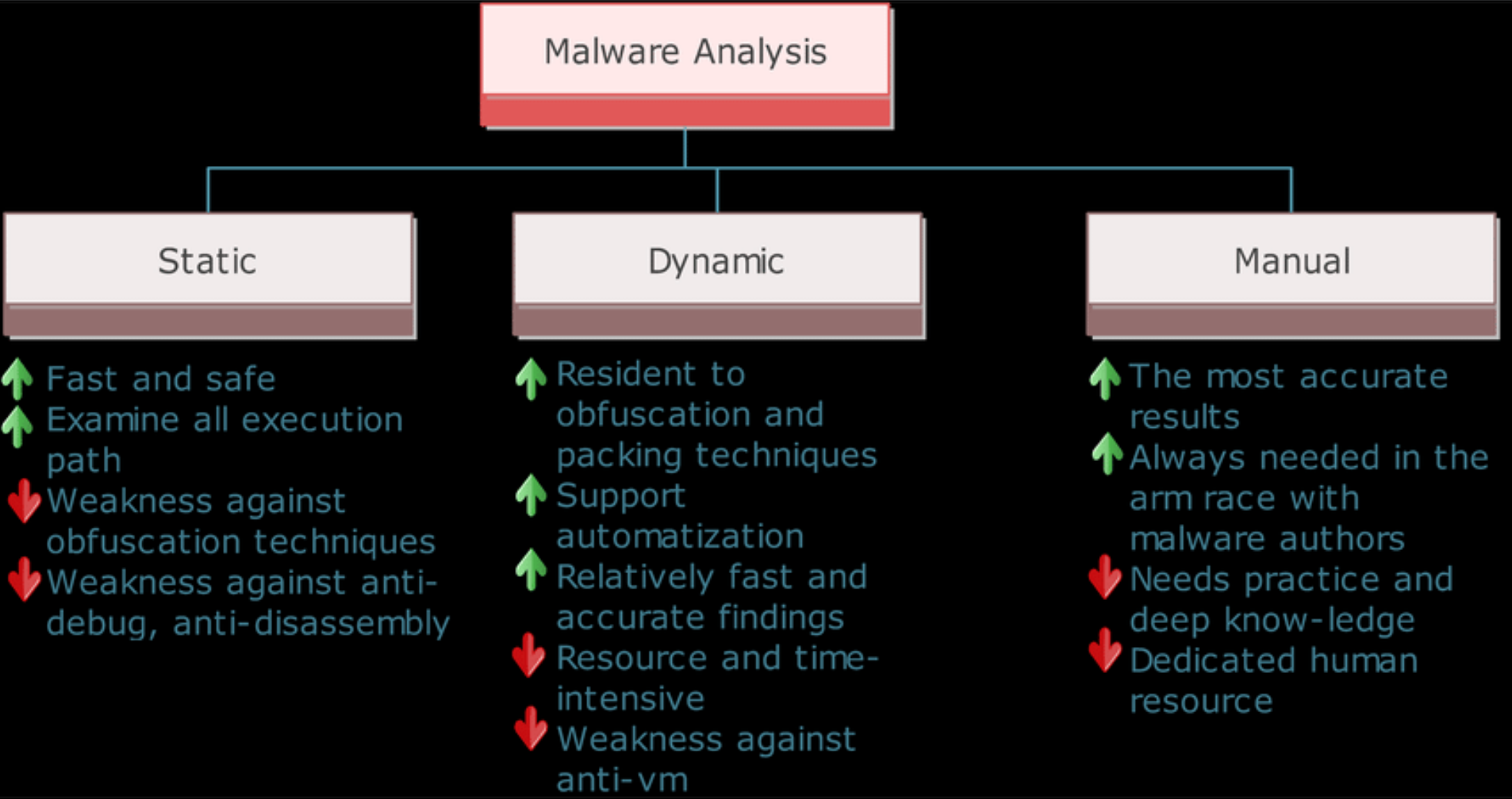
Krypton Zambia

7 tháng 1, 2022 · 🌐



#Malware_analysis
Cuckoo 3 is a Python 3 open source automated malware analysis system
<https://github.com/cert-ee/cuckoo3>
ZLoader Campaign Exploiting Signature Verification Bug
<https://research.checkpoint.com/.../can-you-trust-a-files...>
Code Reuse in the Malware Landscape
<https://isc.sans.edu/.../Code+Reuse+In+the+Malware.../28216>
Agent Tesla Updates
<https://isc.sans.edu/.../Agent+Tesla+Updates+SMTP.../28190>
Malicious Telegram Installer Drops Purple Fox Rootkit
<https://blog.minerva-labs.com/malicious-telegram...>
Skrull - A Malware DRM, That Prevents Automatic Sample Submission By AV/EDR and Signature Scanning From Kernel
<https://github.com/aaaddress1/Skrull>
Labs for Practical Malware Analysis & Triage
<https://github.com/HuskyHacks/PMAT-labs>
Quasar RAT
<https://sfkino.tistory.com/80>
Analyzing an IcedID Loader Document
<https://forensicitguy.github.io/analyzing-icedid-document>
Anti-virus artifacts. Listing APIs hooked by: Avira, BitDefender, F-Secure, MalwareBytes, Norton, TrendMicro, WebRoot
<https://github.com/ethereal-vx/Antivirus-Artifacts>
Malicious npm Packages Are After Your Discord Tokens - 17 New Packages Disclosed
<https://jfrog.com/.../malicious-npm-packages-are-after...>
BRATA - Mobile banking fraud
<https://www.cleafy.com/.../mobile-banking-fraud-brata...>
Ploutus ATM Malware Case Study: Automated Deobfuscation of a Strongly Obfuscated .NET Binary
<https://www.crowdstrike.com/.../ploutus-atm-malware...>
How to Deobfuscate Maze Ransomware
<https://www.crowdstrike.com/.../maze-ransomware...>

Xem bản dịch



👍🥰 Bạn và 28 người khác

9 lượt chia sẻ



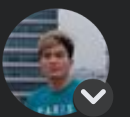
Thích



Bình luận



Chia sẻ



Viết bình luận...

